ABSTRACT

Security Protocol

A security protocol entity (20) is provided that includes a mechanism for enabling a first party (11) to communicate securely with a second party (60) through an access-controlling intermediate party (13) by nesting within a first security session (64) established with the intermediate party (13) a second security session (65) with the second party (60). The protocol data units, PDUs, associated with the second security session (65) are encapsulated in PDUs associated with the first security session (64) when sent out by the first party, the intermediate party extracting the encapsulated PDUs for sending on to the second party (possibly with a change to the destination address included in the PDU to be sent on). Each PDU includes a message type field explicitly indicating to the intermediate party (13) if a received PDU encapsulates another PDU intended to be sent on. The establishment of a security session between two parties is made dependent on each party proving by attribute certificates that it has certain attributes required of it by the other party. Where the intermediate party (13) fronts for the second party (60) and the first party (11) initially contacts the intermediate party in the belief that it is the second party, then the latter will indicate its relay status to the first party which can then request the intermediate party (13) to permit a tunnel to be established through it to the second party (60). The first party may place different attribute requirements on the intermediate party in its tunnel role to those initially expected of it when the first party thought it was the second party.

(Fig. 12)